

**Japan Patent Office,
Unexamined Patent Application Publication No. H7-200756**

PUBLICATION DATE: August 4, 1995

[TITLE OF THE INVENTION]

PORTABLE TYPE DATA CARRIER PROCESSING SYSTEM

[Object] To prevent the illegal use of a security card extracted during a session.

[Constitution] Write completion information indicating the successful completion of a session to security card 30 for authenticating user card 20. In a case that security card 30 is extracted illegally during the session, completion information remains in "incompletion". A host terminal prevents access to data even if security card 30 is inserted in the host terminal; as a result, the illegal use of the card is prevented beforehand.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平7-200756

(43) 公開日 平成7年(1995)8月4日

(51) Int.Cl.⁶

G 0 6 K 17/00

識別記号

庁内整理番号

S

F I

技術表示箇所

審査請求 未請求 請求項の数1 F D (全 5 頁)

(21) 出願番号 特願平5-349861

(22) 出願日 平成5年(1993)12月28日

(71) 出願人 000003193

凸版印刷株式会社

東京都台東区台東1丁目5番1号

(72) 発明者 由良 彰之

東京都台東区台東一丁目5番1号 凸版印刷株式会社内

(72) 発明者 高橋 正志

東京都台東区台東一丁目5番1号 凸版印刷株式会社内

(72) 発明者 松村 秀一

東京都台東区台東一丁目5番1号 凸版印刷株式会社内

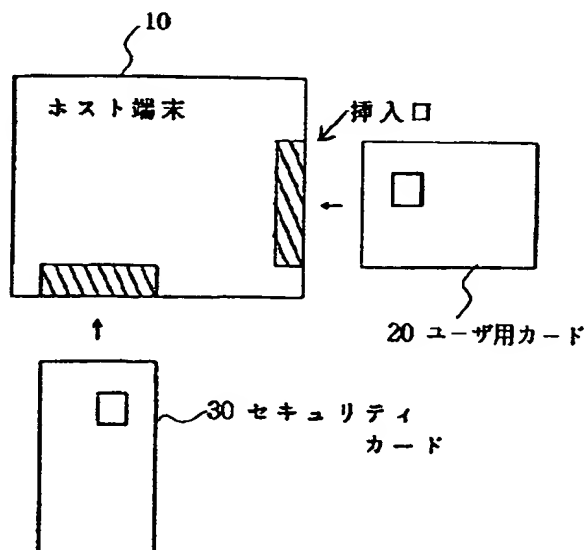
(74) 代理人 弁理士 安倍 逸郎

(54) 【発明の名称】 可搬型データ担体処理システム

(57) 【要約】

【目的】 セッション途中で抜き取られたセキュリティカードの不正使用を防止する。

【構成】 ユーザ用カード20の認証等を行うセキュリティカード30に、セッションの正常終了を表す終了情報を書き込む。セッションの途中でセキュリティカード30が不正に抜き取られた場合には、終了情報は「未終了」のままとなる。このセキュリティカード30をホスト端末に挿入したとしても、ホスト端末はデータのアクセスを禁止するため、不正使用を未然に防止することができる。



【特許請求の範囲】

【請求項1】 可搬型データ担体と、

可搬型データ担体の認証を行った後に可搬型データ担体に対してデータのアクセスを行うホスト端末とを備えた可搬型データ担体処理システムにおいて、

上記可搬型データ担体は終了情報記憶手段を備え、ホスト端末は以下の(1)～(4)の処理を実行することを特徴とする可搬型データ担体処理システム。

(1)ホスト端末が可搬型データ担体を認証した場合には、ホスト端末は終了情報記憶手段に「未終了」のデータを書き込む。

(2)可搬型データ担体に対するデータのアクセスが正常に終了した場合には、ホスト端末は終了情報記憶手段に「終了」のデータを書き込む。

(3)ホスト端末が可搬型データ担体を認証する際に終了情報記憶手段に「終了」のデータが書き込まれていた場合には、ホスト端末は可搬型データ担体に対するデータのアクセスを許容する。

(4)ホスト端末が可搬型データ担体を認証する際に終了情報記憶手段に「未終了」のデータが書き込まれていた場合には、ホスト端末は可搬型データ担体に対するデータのアクセスを禁止する。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、可搬型のデータ担体処理システム、詳しくは移動通信等において使用されるSIM (Subscriber Identity Module)、金融アプリケーションにおけるSAM (Secure Application Module)、もしくはICカード等の可搬型データ担体処理システムに関する。

【0002】

【従来の技術】近年、移動通信、金融アプリケーション等の分野においては、持ち運び容易なSIM、SAM、ICカード等の可搬型データ担体が使用されている。例えば、金融アプリケーション等の分野において使用が検討されているSAMは、セキュリティを必要とするアプリケーションプログラムの一部、例えば暗号・復号プログラムが書き込まれたICカード等の可搬型データ担体であって、一般ユーザ使用のカードとは別のものである。

【0003】このような可搬型データ担体は、ホスト端末の挿入口に差し込まれ、両者の鍵が一致するか否かを判断することにより可搬型データ担体の正当性が確認される。そして、可搬型データ担体が正当であると認証された場合には、ホスト端末においてセッション等のデータのアクセスが行われる。このとき、可搬型データ担体には、正当な認証が行われたことを表すデータ、認証用のKeyデータ、乱数のデータ等が書き込まれる。

【0004】しかしながら、セッションが終了する前

に、可搬型データ担体をホスト端末から抜き取った場合には、可搬型データ担体は正当であると認証された状態のままである。したがって、抜き取られた可搬型データ担体を他のホスト端末等に挿入した場合、このホスト端末においてデータのアクセスが許可されてしまう。すなわち、可搬型データ担体等のセキュリティ機能の部分のみを不正に抜き取られた場合、他のホスト端末において不正使用されるおそれが生じる。すなわち、この可搬型データ担体をホスト端末に挿入した際に、認証用のKeyデータ、乱数のデータの交換等がされることなく、セッションが行われてしまう。金融アプリケーション等においては、このような問題は特に重大である。

【0005】

【発明の目的】そこで、本発明は、可搬型データ担体処理システムにおいて、セッションの途中において抜き取られた可搬型データ担体の不正使用を禁止することを目的としている。

【0006】

【課題を解決するための手段】請求項1に記載の発明は、図1に示されるように、可搬型データ担体1と、可搬型データ担体の認証を行った後に可搬型データ担体に対してデータのアクセスを行うホスト端末2とを備えた可搬型データ担体処理システムにおいて、上記可搬型データ担体は終了情報記憶手段3を備え、ホスト端末2は以下の(1)～(4)の処理を実行することを特徴とする可搬型データ担体処理システムである。

【0007】(1)ホスト端末2が可搬型データ担体1を認証した場合には、ホスト端末2は終了情報記憶手段3に「未終了」のデータを書き込む。(2)可搬型データ担体1に対するデータのアクセスが正常に終了した場合には、ホスト端末2は終了情報記憶手段3に「終了」のデータを書き込む。(3)ホスト端末2が可搬型データ担体1を認証する際に終了情報記憶手段3に「終了」のデータが書き込まれていた場合には、ホスト端末2は可搬型データ担体1に対するデータのアクセスを許容する。

(4)ホスト端末2が可搬型データ担体1を認証する際に終了情報記憶手段3に「未終了」のデータが書き込まれていた場合には、ホスト端末2は可搬型データ担体1に対するデータのアクセスを禁止する。

【0008】

【作用】請求項1に記載の発明において、ホスト端末が可搬型データ担体を認証した場合には、ホスト端末は終了情報記憶手段に「未終了」のデータを書き込む。そして、正当権限者による非活性化命令によって可搬型データ担体に対するデータのアクセスが正常に終了した場合には、ホスト端末は終了情報記憶手段に「終了」のデータを書き込む。このようにして正当な権限者により正常終了した可搬型データ担体を、再度ホスト端末に挿入したとする。この場合には、終了情報記憶手段に「終了」のデータが書き込まれているため、ホスト端末は可搬型

データ担体に対するデータのアクセスを許容する。一方、データのアクセスが正常に終了する前に可搬型データ担体を不正に抜き取った場合には、終了情報は「未終了」の状態のままである。したがって、この可搬型データ担体を再度ホスト端末に挿入した場合、ホスト端末は可搬型データ担体に対するデータのアクセスを一切禁止し、可搬型データ担体の使用は不可能になる。これにより不正に抜き取られた可搬型データ担体を利用した不正行為を未然に防止することができる。

【0009】

【実施例】以下に、本発明の一実施例を図面を参照しながら説明する。

【0010】図2は本実施例に係る可搬型データ担体処理システムの外観構成図である。この可搬型データ担体処理システムは、ホスト端末10、ユーザ用カード20、セキュリティカード30を備えて構成されている。ホスト端末10は、ユーザ用カード20に対してデータの読み書きを行うものであって、暗号化・復号化および認証処理等を実行するCPU、アプリケーションプログラム等が書き込まれたメモリ等により構成されている。また、ホスト端末10には、ユーザ用カード20、セキュリティカード30が挿入される挿入口を備えている。

【0011】ユーザ用カード20は、金融情報等のデータを保持するものであって、データの暗号化・復号化等を行うマイクロコンピュータおよびトランザクションファイル等を記憶する不揮発性メモリ等を内蔵している。このユーザ用カード20は各ユーザが所持するものである。

【0012】セキュリティカード30もまた、マイクロコンピュータおよび不揮発性メモリを備えて構成されている。このセキュリティカード30は、主としてサービスを提供する者が所持するもので、ホスト端末10に挿入されたユーザ用カード20が正当なものであるか否か、また、ホスト端末10が受信したデータが正当であるか否かを確認する機能を備えている。不揮発性メモリは、電氣的消去可能なEEPROM、あるいは、バッテリバックアップされたスタティックRAM等により構成されている。また、セキュリティカード30には、外部からアクセス不可能な不揮発性メモリを備え、この不揮発性メモリには後述する終了情報が書き込まれている。終了情報は、前回のセッション中においてセキュリティカード30が不正に抜き取られた場合には「未終了」の状態となるものである。よって、この終了情報を確認することによりセキュリティカード30の不正使用を防止することが可能となる。

【0013】なお、セキュリティカード30と同等の機能を、図3のセキュリティ処理装置40として実現することも可能である。セキュリティ処理装置40はホスト端末10にインタフェース等を介して接続されており、ホスト端末10から切り離すことが可能なものである。

【0014】図4は、本実施例に係る可搬型データ担体処理システムにおける処理の概要を表す図である。相互認証は、ユーザ用カード20が正当なものであるか否かを確認する処理であり、この相互認証は、端末ホスト10がユーザ用カード20およびセキュリティカード30のそれぞれの暗号化したデータ(鍵)等が一致するか否かにより行われる。また、ユーザ用カード20は、取引に伴い電子署名を生成し、この電子署名はセキュリティカード30により確認される構成となっている。

【0015】以上のように構成された可搬型データ担体処理システムの作用を図5に示されるフローチャートを参照しながら説明する。

【0016】サービス提供者がセキュリティカード30をホスト端末10の挿入口に挿入すると、ホスト端末10からセキュリティカード30に電源が供給され、セキュリティカード30が活性化する(S1)。次に、ホスト端末10は、セキュリティカード10に記録された終了情報が「終了」を表しているか否かを確認する(S2)。

【0017】この終了情報は、前回のセッションが正常に終了したか否かを表すフラグであって、セッションが正常に終了しないうちにセキュリティカード30をホスト端末10から引き抜いた場合には終了情報は「未終了」の状態のままとなる。ホスト端末10は、読み取った終了情報が「未終了」であった場合(S2でNO)には、一切応答することなく以後のアクセスを禁止する(S3)。これにより、セッション途中で抜き取られ、認証された状態のままのセキュリティカード30を利用した不正使用を防止することができる。なお、無応答の処理は、無限ループ等を利用することにより実現可能である。一方、終了情報が「終了」であった場合(S2でYES)には、ホスト端末10は、セキュリティカード30内の終了情報を「未終了」に書き換え(S4)、ステップS5以後の処理を実行する。

【0018】ステップS5において、ホスト端末10はコマンドの送信をセキュリティカード30に許可し、コマンドが送信されてくるのを待機する。ホスト端末10が、コマンドを受信すると(S6でNO)、受信したコマンドが非活性化命令のコマンドであるか否かを判断する(S7)。非活性化コマンドでない場合(S7でNO)には、セッションコマンド等の処理を実行し(S13)、レスポンスを送信する(S14)。そして、再び、ホスト端末10は新たなコマンドが送信されてくるのを待機する(S5)。一方、ステップS7において、ホスト端末10が非活性化コマンドを受信した場合(S7でYES)には、このコマンドとともに受信した鍵とセキュリティカード30内の参照鍵とを照合する(S8)。

【0019】両者が一致しなかった場合(S9でNO)には、ホスト端末10は、一致しなかった旨のレスポンス

スを送信し（S14）、新たなコマンドを待機する（S5）。両者が一致した場合（S9でYES）には、上述した終了情報を「終了」に書き換える（S10）。そして、ホスト端末10は、レスポンスを送信した後（S11）、セキュリティカード30を非活性化し（S12）、全ての処理を終了する。

【0020】したがって、本実施例によれば、終了情報を参照することにより、セキュリティカード30がセッション途中で抜き取られたものか否かを判断でき、このセキュリティカード30を利用した不正使用を未然に防止することが可能となる。なお、図3に示すように、セキュリティカード30と同等の機能を有するセキュリティ処理装置40について本発明を適用することも可能である。また、ホスト端末10の内部にセキュリティ処理装置40が配設されている場合においても、セキュリティ処理装置40を切り離し、不正使用することも考えられることから、このような場合にも本発明を有効に適用することができる。

【0021】

【発明の効果】以上説明してきたように、本発明によれば、可搬型データ担体処理システムにおいて、セッションが正常に終了したか否かを表す終了情報を確認することにより、セッション途中で抜き取られた可搬型データ担体の不正使用を未然に防止することが可能となる。

【図面の簡単な説明】

【図1】本発明に係る可搬型データ担体処理システムを表すブロック図である。

【図2】本発明の一実施例に係る可搬型データ担体処理システムのブロック図である。

【図3】本発明の一実施例に係る可搬型データ担体処理システムのブロック図である。

【図4】本発明の一実施例に係る可搬型データ担体処理システムのデータの流を表す図である。

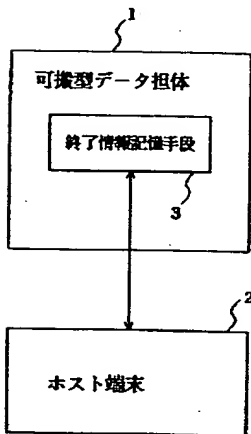
【図5】本発明の一実施例に係る可搬型データ担体処理システムの作用を表すフローチャートである。

【符号の説明】

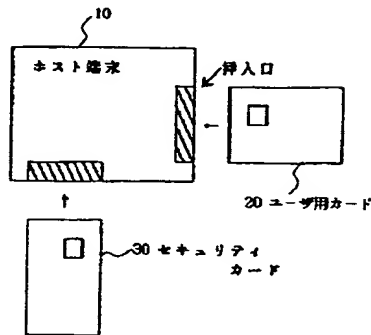
10 ホスト端末

30 セキュリティカード（可搬型データ担体）

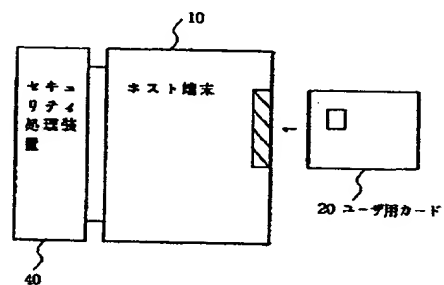
【図1】



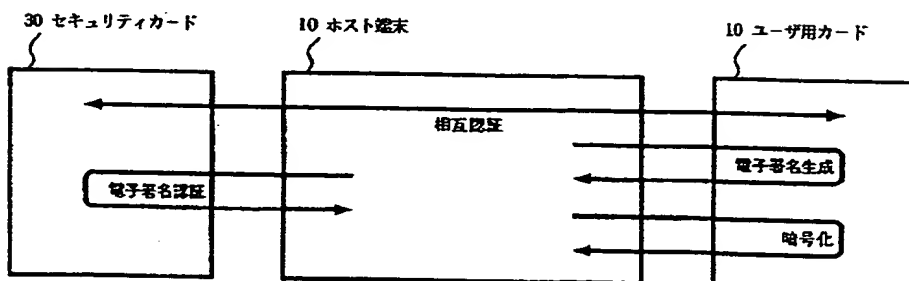
【図2】



【図3】



【図4】



【図5】

